Security Incident Trends

Carrianne J. Zimmerman
Office of Security Enforcement
Office of Enforcement

April 6, 2011

Contractor Trending and Analysis Purpose

- **Know and Understand Your Security Data**
- **Provide a Basis for Management in Making Risk Based Decisions**
  - Self-reporting noncompliant conditions
  - Specific topics to be addressed during assessment activities
  - Rigor of causal/root cause analysis
  - Effectiveness of implemented corrective actions
  - Areas requiring management attention
- **Identify and Correct Precursor Noncompliances Before a Major Event Occurs (Proactive vs. Reactive)**

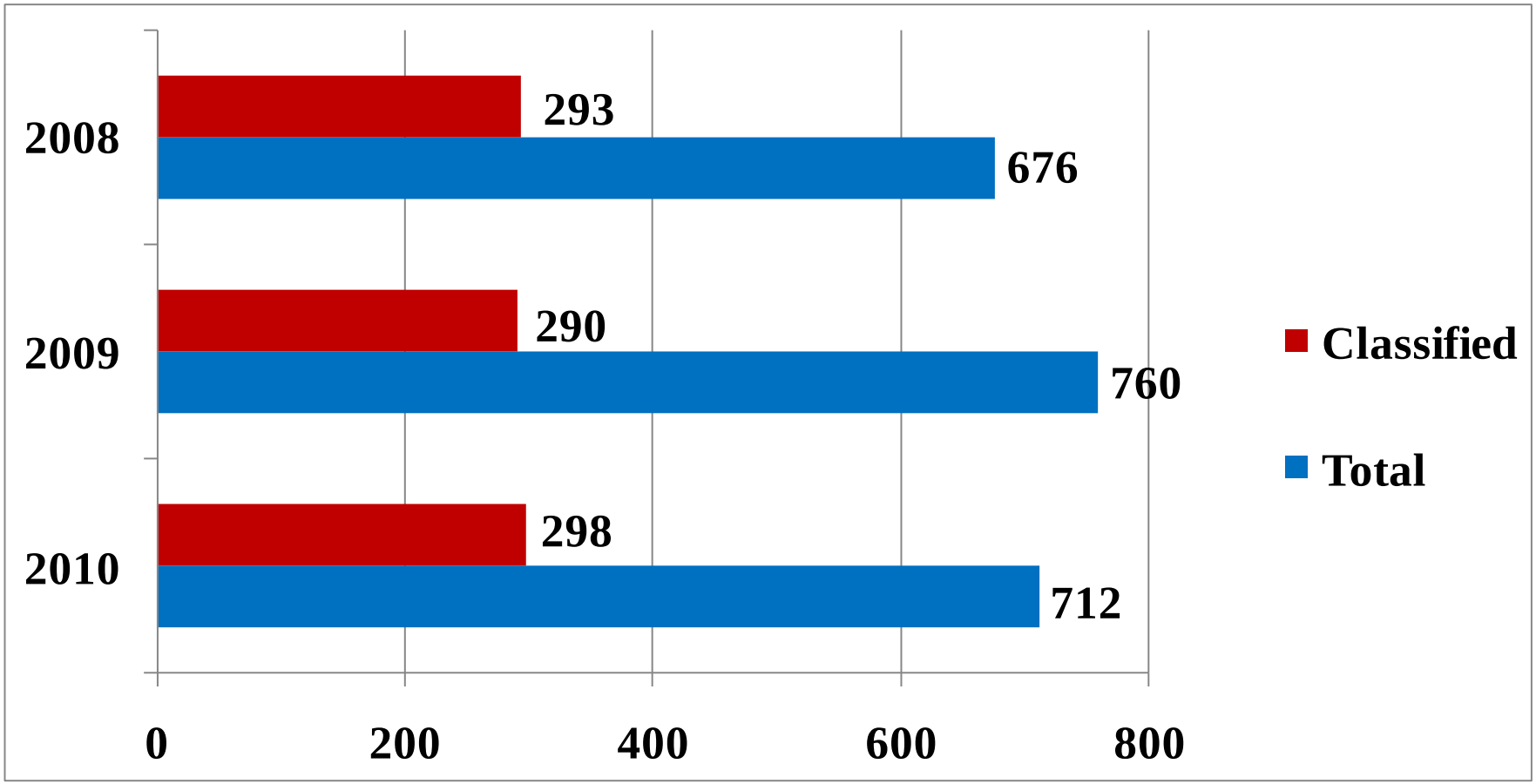
Elements of Effective Contractor Trending and Analysis

- **Data is Easily Accessible and not Compartmentalized**
  - Security incident data
  - Internal/external Assessments (e.g., Self-Assessments, Surveys, Inspections, IG, GAO) Results
- **Look Beyond Numbers (e.g., Stick Counts or IMI Categories)**
  - Who, What, When, Where, How, and How Often
  - Classified Subjects, Locations, Organizations, Employees, Programs, etc.
  - System Failures vs. Human Issues

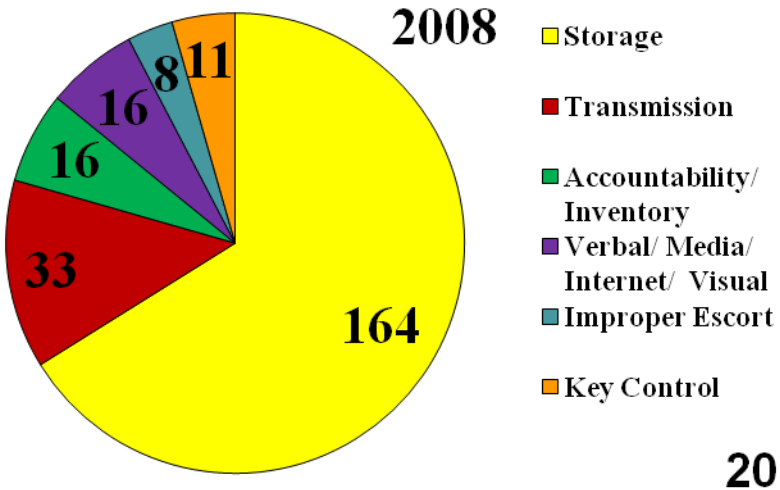
Elements of Effective Contractor Trending and Analysis (cont'd)

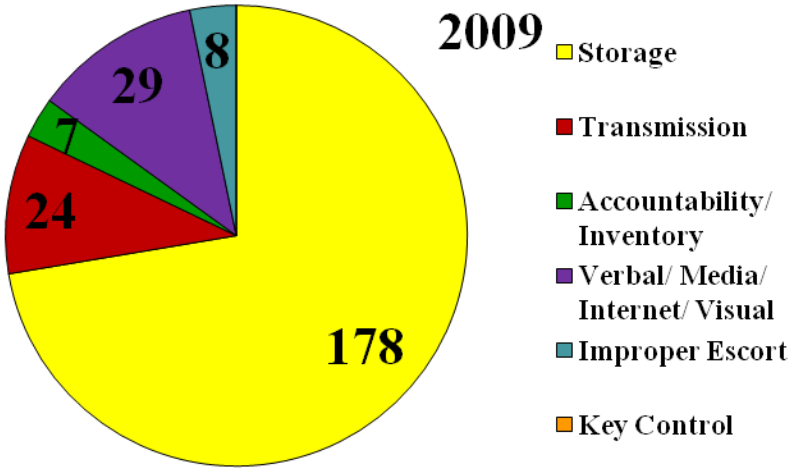
- **Conduct Comprehensive Analysis of Identified Trends**
  - Root Cause Themes
  - Extent of Conditions
- **Implement Sustainable Corrective Actions**
  - Engineered Controls vs. Administrative Procedures

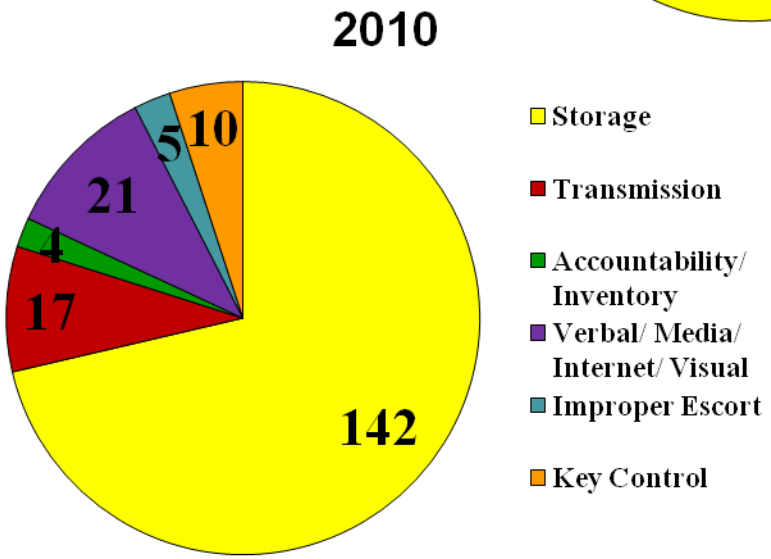
Total Incidents and Incidents Involving Classified Information



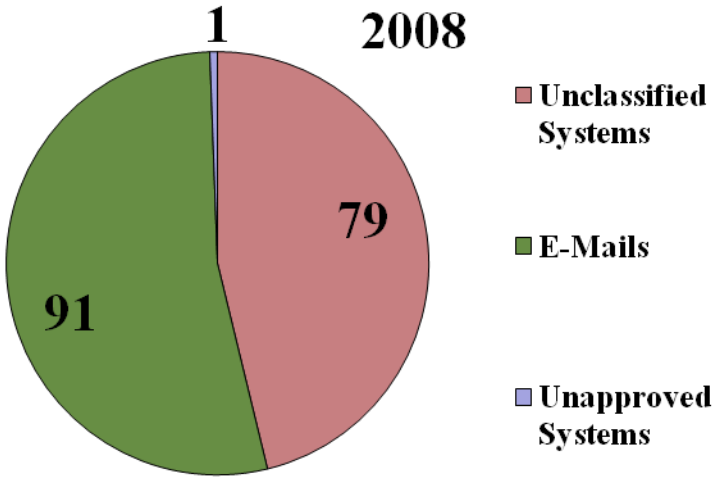
Handling & Storage

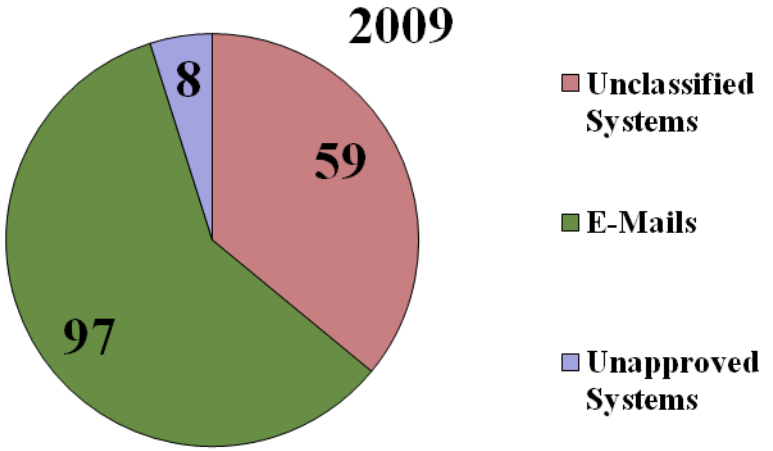


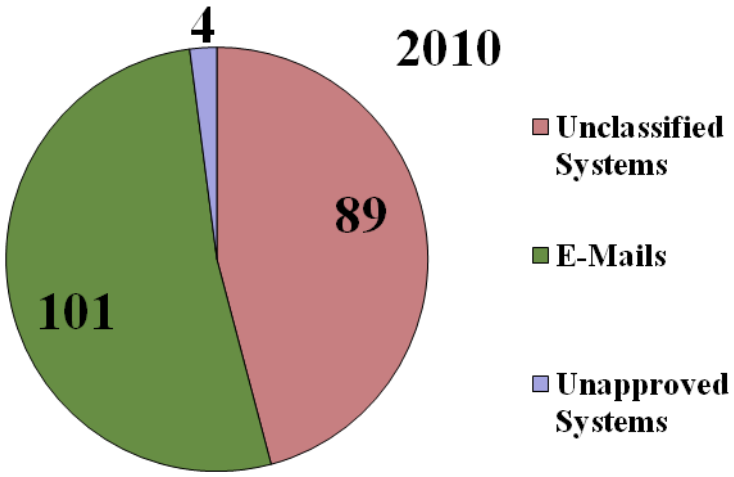




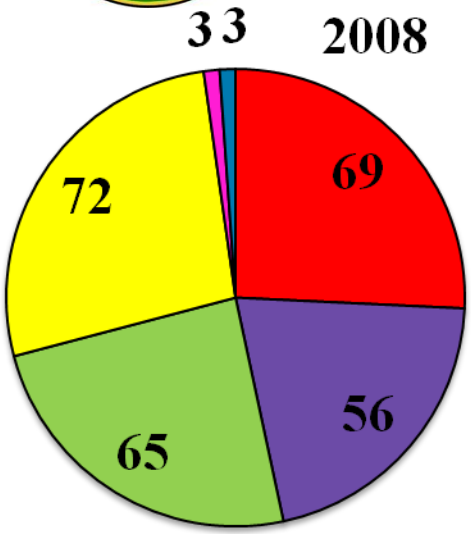
Cyber Related Incidents

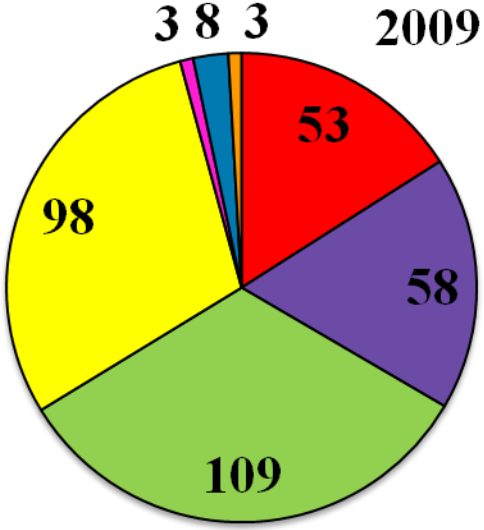


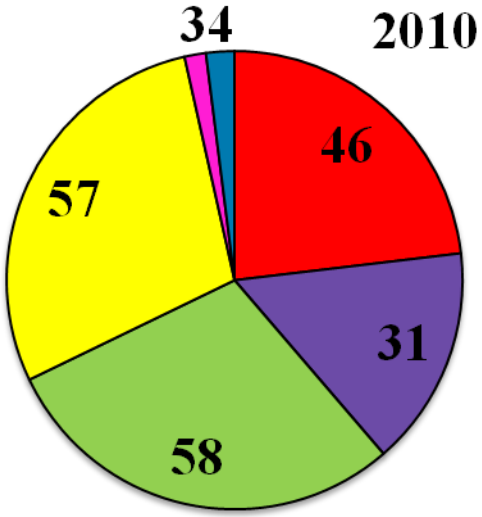




Corrective Actions







- Disciplinary Actions
- Coaching/ Counseling
- Policy/ Procedural Changes
- Training Modifications
- Cyber System Modifications
- Physical System Modificaitons
- Communication System Modifications

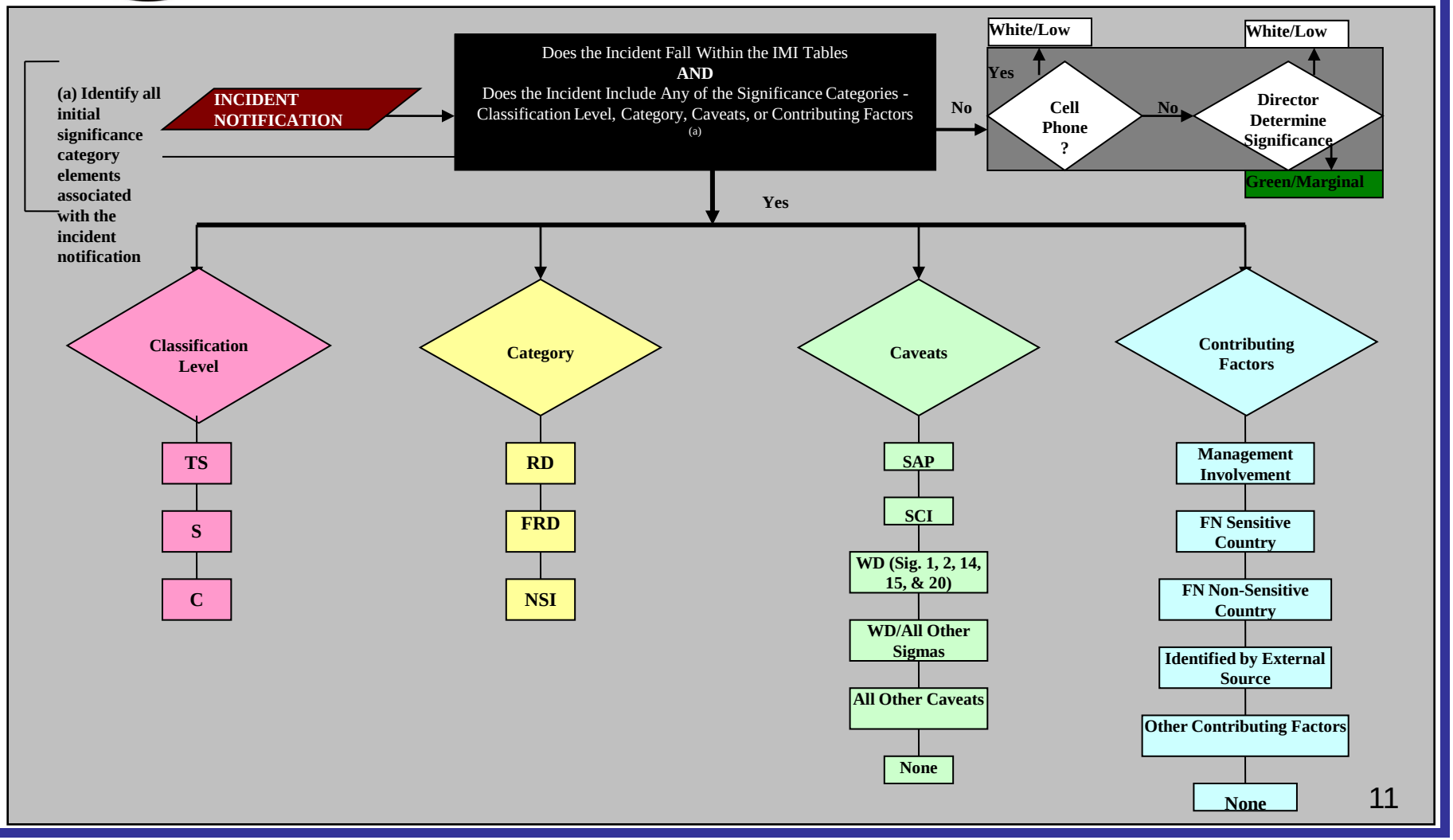
Office of Security Enforcement Trending and Analysis

- **Security Significance Database Purpose**
  - Tool to Evaluate Security Significance of Reportable Incidents (Risk Based Decisions)
  - Contractor Organizations are Evaluated in a Consistent Manner
  - Provides Valuable Trending Information (i.e., Dashboards, Specific Reports, and Graphs)

Office of Security Enforcement Trending and Analysis (cont'd)

- **Security Significance Database Methodology**
  - Numerical Value Assigned to Each Established Factor
  - Assigns an Overall Numerical Significance Value
  - Determines the Appropriate Significance Range (i.e., High, Serious, Medium, Low)
  - Measures Each Incident and Provides an Aggregate Score

Office of Security Enforcement Trending and Analysis



Office of Security Enforcement Trending and Analysis

HSS
Office of Health, Safety and Security